



CVE-2010-1446

Published on: 05/21/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:18 AM UTC

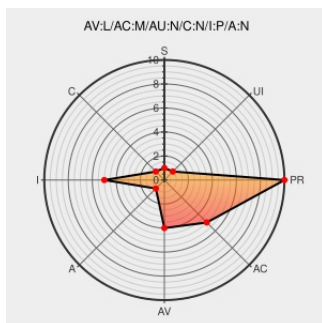
CVE-2010-1446

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

arch/powerpc/mm/fsl_booke_mmu.c in KGDB in the Linux kernel 2.6.30 and other versions before 2.6.33, when running on PowerPC, does not properly perform a security check for access to a kernel page, which allows local users to overwrite arbitrary kernel memory, related to Fsl booke.

CVE-2010-1446 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **1.9 - LOW**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Debian -- Security Information -- DSA-2053-1 linux-2.6

www.debian.org
Deprecated Link
text/html

[DEBIAN DSA-2053](#)

oss-security - Re: CVE request - Linux Kernel KGDB/ppc issue

www.openwall.com
text/html

[MLIST \[oss-security\] 20100429 Re: CVE request - Linux Kernel KGDB/ppc issue](#)

oss-security - CVE request - Linux Kernel KGDB/ppc issue

www.openwall.com
text/html

[MLIST \[oss-security\] 20100429 CVE request - Linux Kernel KGDB/ppc issue](#)

Security Advisory SA40645 - SUSE update for kernel - Secunia

web.archive.org
text/html

[SECUNIA 40645](#)

Debian update for linux-2.6 - Advisories - Community

web.archive.org
text/html

[SECUNIA 39830](#)

LKML: Greg KH: [071/117] kgdb: dont needlessly skip PAGE_USER test for Fsl booke	Patch lkml.org text/xml	 MLIST [linux-kernel] 20100510 [071/117] kgdb: dont needlessly skip PAGE_USER test for Fsl booke
oss-security - Re: CVE request - Linux Kernel KGDB/ppc issue	www.openwall.com text/html	 MLIST [oss-security] 20100430 Re: CVE request - Linux Kernel KGDB/ppc issue
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	lists.opensuse.org text/html	 SUSE SUSE-SA:2010:031
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF kernel-kgdb-memory-overwrite(58840)
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2010-1857

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	All	All	All
Operating	Linux	Linux Kernel	2.6.31.1	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.31.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.5	All	All	All
Operating	Linux	Linux Kernel	2.6.32.6	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.32.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.4	All	All	All

Operating System	Linux	Linux Kernel	2.6.31.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.32.9	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.30:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.2:*:*:*:*:*:						

cpe:2.3:o:linux:linux_kernel:2.6.30.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.3:*****:

cpe:2.3:o:linux:linux_kernel:2.6.32.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.6:*****:

cpe:2.3:o:linux:linux_kernel:2.6.31.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)